Response to PTLO dated 11/03/2005 from Bill Dean

As Requested the Abstract has been separated onto its own sheet of paper. Note that there are no changes or alterations to the abstract.

The claims are on 4 sheets following the Abstract. Claims 1 & 3 through 29 are not changed or altered.

Claim 2 has no deletions and the addition of the words "that are downloaded from the communicant's internet web site" in this claim are now underlined instead of circled.

The concept of this change can be found in figure 4a and description paragraph 65. The description paragraphs have no changes or alterations. The figures have no changes or alteration. Below is included a copy of paragraph 65 for you convenience and on the following page you will find a copy of figure 4a. As you can see below "and at the same time will read the compiled lists of identification numbers from such home page" reflects the additions I propose to claim 2.

[0065] If the called party 14 has created a home page 38 having the gatekeeper program installed, as shown in FIG. 4a, the caller's browser will then read the HTML instructions from the home page, and at the same time will read the compiled lists of identification numbers from such home page. A screen will then appear similar to the one shown in FIG. 6 wherein superimposed over home page 38 is a box 94 prompting caller 12 to enter his or her ten digit home telephone number. Box 94 will preferably appear any time a call is made to a telephone number or address having one or more restricted access commands of the gatekeeper program activated.

Hopefully this will address your concerns of you 11-3-2005 PTLO Response

Thanks
Kevin P. Ryan
10/075,573
610-965-0835
6402 Ridge Road
Zionsville, PA 18092
kevinryan@enter.net

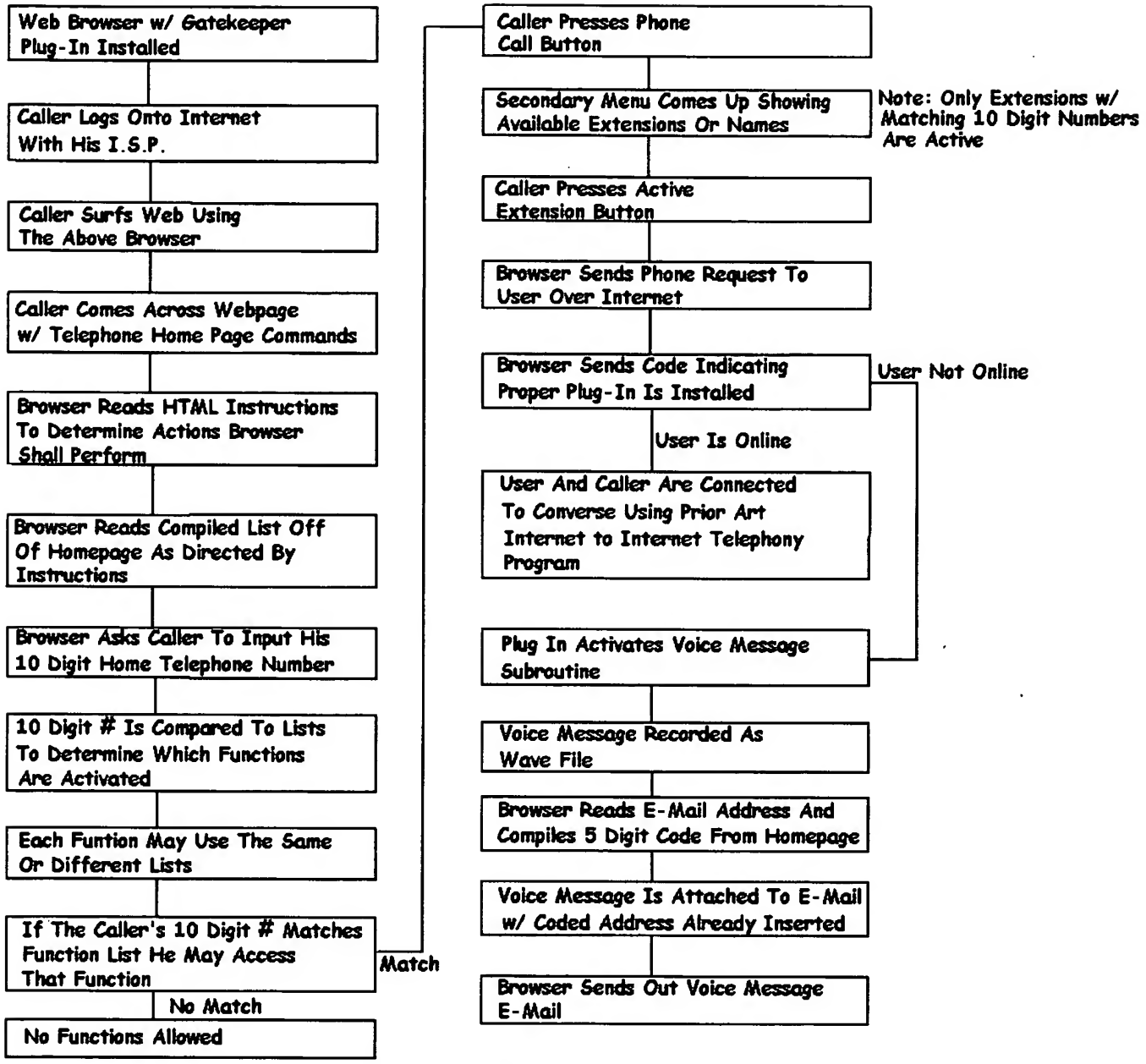
Web Browser w/ Gatekeeper Plug-In Installed
Caller Logs Onto Internet With His I.S.P.
Caller Surfs Web Using The Above Browser
Caller Comes Across Webpage w/ Telephone Home Page Commands
Browser Reads HTML Instructions To Determine Actions Browser Shall Perform
Browser Reads Compiled List Off Of Homepage As Directed By Instructions
Browser Asks Caller To Input His 10 Digit Home Telephone Number
10 Digit # Is Compared To Lists To Determine Which Functions Are Activated
Each Funtion May Use The Same Or Different Lists
If The Caller's 10 Digit # Matches Function List He May Access That Function
Match
No Match
No Functions Allowed
Caller Presses Phone Call Button
Secondary Menu Comes Up Showing Available Extensions Or Names
Note: Only Extensions w/ Matching 10 Digit Numbers Are Active
Caller Presses Active Extension Button
Browser Sends Phone Request To User Over Internet
Browser Sends Code Indicating Proper Plug-In Is Installed
User Not Online
User Is Online
User And Caller Are Connected To Converse Using Prior Art Internet to Internet Telephony Program
Plug In Activates Voice Message Subroutine
Voice Message Recorded As Wave File
Browser Reads E-Mail Address And Compiles 5 Digit Code From Homepage
Voice Message Is Attached To E-Mail w/ Coded Address Already Inserted
Browser Sends Out Voice Message E-Mail

Figure 4A

Why Claims in Ryan Application Are Unique to Randall Application Telecommunication & Cellular Homepage Call Screening Control Center.

The method of screening and authentication in the Randall Application can be found in paragraphs [0067] & [0068].

My contention is that the authentication logic listed in Randall is not unique in that the same logic is already used in common screening/authentication devices commonly used today.

Randall Logic
A) The user wishes to control access at a remote location.

B) The device at the remote location has sensitive data and must have verification that the user is allowed access to the data.

C) The user must verify his identity to a server before the server allows access to remote data.

D) The server requires a code or PIN from the user or the user's device verifying the user is an allowed person.

E) The server checks the PIN against a list of internally stored PINS to verify allowed access.

This verification logic already exists today in common technology such as e-mail access and ATM Bank machines. Let's look at how you are currently granted access to e-mails at your internet provider.

E-mail Screening Logic
a) You need access to e-mails sent to you stored on a hard drive at your providers site.

b) Your e-mails are private and therefore your identity must be verified before access to this hard drive is allowed.

c) Your internet provider's server must verify your identity before access is allowed to protect your privacy.

d) Your internet provider's server requires a code or PIN from you or that code or pin must be stored on your computer verifying you are who you say you are.

e) Your internet provider's server checks the pin against a list of internally stored PINS to verify your access to the remote hard drive.

As you can see the information accessed and devices in the 2 examples above may be different, but the procedure for authentication is basically identical.

The screening process claimed in the Ryan Application has two additional steps that are required in addition to authentication steps listed above and is unique by the nature of the additional steps required.

Additional Step 1
The server that screens the calls must have access to the internet and retrieve a compiled list of allowable codes that are stored on a public accessible web site. Access to the site is available to the public through normal internet surfing procedures; therefore the codes must be compiled/encrypted. The server that screens the calls must then unencrypt the codes to proceed with comparison of PINs/Codes.

This step in itself makes the screening process unique from the Randall Application and current common technology used to identify users of electronic devices. This process gives the person screening the calls the ability to have direct access to their own verification codes on their own web site giving them more flexibility in control of their incoming communications.

In claims 26 through 28 of the Ryan Application the server providing the screening process resides at a remote location from the cell phone caller and therefore the user would not have access to modify the program screening the user. In this iteration of the invention only step one is required to screen calls in addition to the original 5 steps listed above.

However when the server screening the calls is the users own computer then a second step is required to insure proper screening. The user could modify the existing program or buy a new program that would bypass the screening process and make the phone connection regardless of PIN/code matching, since he is in control of the server that is screening the calls.

Additional Step 2
The person who is receiving communication must also have a compatible program to verify that the caller did not bypass the screening process by providing his own screening program. The receiving parties device will detect a manufacturer code sent with the communication to verify that the communication is from a device using proper screening procedures. If this code is not received with the communication the receiver's device will not ring through to the receiver.

In the case of e-mails, the user's device will add a code to the end the e-mail address that appears as unreadable to the users. (example kryan@ptd.net*****) If the e-mail is sent without this code the receiver's device will delete the e-mail without the receiver ever seeing it.

These two additional steps are explained in paragraphs [0066] & [0067] of the Ryan Application and are the basis for this patent.

Understanding that although this screening procedure is documented in the application, you were concerned that the claims did not properly express additional step1 required that makes this invention unique. Therefore, I might suggest the following additions to the claims to clarify the unique features of the invention if these changes would satisfy your requirements.

2) The system for enabling a communicant to personally control one or more means of communication via the digital data network of claim 1 wherein said means for selectively controlling which communications options are available to an outside party comprises one or more lists of preprogrammed digital codes capable of identifying certain outside parties, each of said one or more lists being associated with one or more of said communications options, and wherein prior to the communications options menu being activated each outside party is required to supply a digital code, which code is compared with the lists or preprogrammed codes **that is downloaded from the communicant's internet web site,** and wherein if said code matches any of the preprogrammed codes the communications options associated with said lists will be activated.

I have included the above changes in the complete list of claims attached with this letter. Hopefully this will satisfy your requirements for allowing this patent.

Below I have attempted to address the other art that you have referenced in your 35 U.S.C. 102 Rejection Letter.

US patent No. 6775264 Kurganov
This invention appears to be a method for a subscriber to have multiple devices access the same data on a server. This inventions does not appear to be an invention to screen others from calling the subscriber. The Ryan application references to fax, e-mail, telecommunications, and other communication processes are only a process to screen these forms of communication and uses existing art to accomplish these tasks once screening has occurred. Therefore, any new form of communication networking attributed by Kurganov would not apply to Ryan application.

US patent No. 6400806 Uppaluru
This invention allows services to be provided to a user by comparing the user's voice print to that of a voice print stored on the web. This invention is not used for screening of others from reaching the user but to identify the user and allow the user to receive services based on his identity.

US patent No. 5940834 Pinard
This invention allows for generation of web based data bases that can be shared by multiple users. Mention of call screening in this patent is only for the purpose of mentioning that call screening references can be stored in the database. This invention does not appear to screen call itself.

US patent Application No 2002/0045456 Obradovich
This invention allows for application to be directed to a user according to location based on GPS information periodically undated from the users device. These applications are based on location and are not screened. This invention also allows requesters to have access to the users website that has updated information on the users location and contact information. This invention screens requesters for access to the web site but does not allow direct communication with the user. The requester must read contact information off the web site and dial manually. The procedure for screening the requester's is not clear therefore comparison to the steps required for screening under Ryan is not possible.

Please feel free to call me if you have any question regarding my application.

Sincerely

Kevin P. Ryan
610-965-0835
www.Kevin-Ryan.com
kryan@ptd.net
Patent Application 10/075,573